Sasha [.] pons [at] gmail [.] com

Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Références
• Guide de l'archivage électronique et du coffre-fort électronique, de la signature électronique et de l'horodatage - Fédération Nationale des Tiers de Confiance (F.N.T.C) - www.fntc.org
• AFNOR NF Z42-013 - « Spécifications relatives à la conception et à l'exploitation de SI en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes »
• AFNOR NF Z74-400 - « Exigences concernant la politique mise en œuvre par les autorités de certification délivrant des certificats qualifiés »
• Non-consultée : AFNOR NF Z 67-147 - « Mode Opératoire de procès-verbal de constat sur Internet effectué par Huissier de Justice » :-/
• RFC3161-Timestamp; RFCs du groupe pkix;
CLUSIF / CLUSIR Rha
Conservation de la preuve
2

Depuis l'an 2000, tous les textes légaux ou réglementaires produits vont dans le même sens : la reconnaissance de la valeur légale des formes électroniques et le formalisme ou les exigences qui sont attachés à leur valeur. Il est désormais impossible d'ignorer ces textes :

• 2000 : Loi du 13 mars 2000 qui introduit l'écrit électronique dans le Code Civil ;

• 2004 : Loi sur la Confiance dans l'Économie Numérique (LCEN) qui complète les

dispositions apportées par la Loi du 13 mars 2000 en autorisant les écrits sous forme

électronique chaque fois qu'un écrit est requis pour la validité d'un acte ;

• 2006 : Instruction fiscale relative au contrôle des comptabilités informatisées (récapitulant

l'ensemble des exigences depuis la loi de finances récapitulative pour 1990) ;

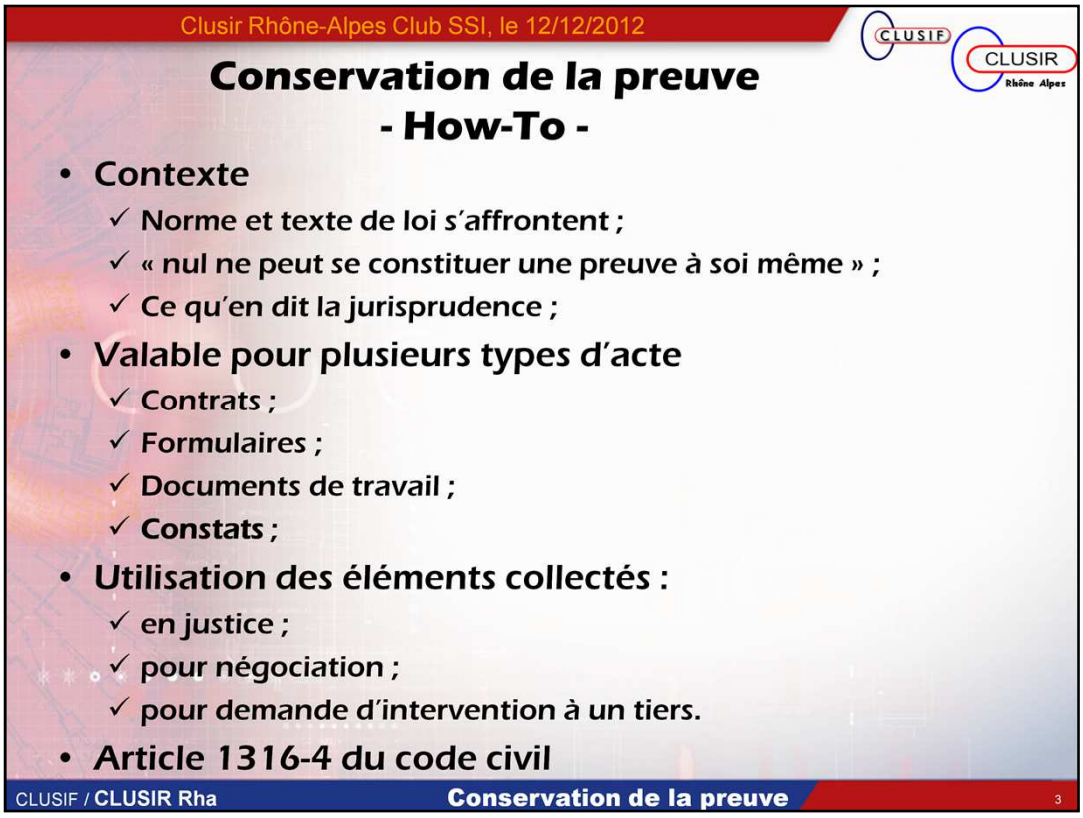
• 2007 : Instruction fiscale relative à la conservation sous forme électronique des copies

de factures produites sur support papier ;

• 2009 : Loi autorisant la dématérialisation du bulletin de paie qui en fixe le cadre et arrêté

du 4 décembre 2009 rendant réglementaire pour l'archivage électronique des collectivités

la norme d’archivage électronique AFNOR NF Z42-013.


Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Conservation de la preuve
- How-To -
• Contexte
✓ Norme et texte de loi s'affrontent ;
✓ « nul ne peut se constituer une preuve à soi même » ;
✓ Ce qu'en dit la jurisprudence ;
• Valable pour plusieurs types d'acte
✓ Contrats ;
✓ Formulaires ;
✓ Documents de travail ;
✓ Constats ;
• Utilisation des éléments collectés :
✓ en justice ;
✓ pour négociation ;
✓ pour demande d'intervention à un tiers.
• Article 1316-4 du code civil
CLUSIF / CLUSIR Rha
Conservation de la preuve
3

Contexte :

§ Norme et texte de loi s'affrontent, notamment sur la **copie** :

D'après NF **Z42-013** :

« Fidélité d'un document : un document est considéré comme fidèle au document d'origine s'il permet de reconstituer toute l'information nécessaire aux usages auxquels le document d'origine était destiné. Ce concept est utilisé en cas de rupture incluant notamment une numérisation ou une conversion de format. »

-> faux : exemple d'une photocopie d'un chèque bancaire pour tirer des espèces au guichet d'une banque, impossible.

Fidélité de la copie, **Article 1348** du code civil :

« Elles reçoivent aussi exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle, mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support. »

-> la loi ne définit pas de critère de fidélité, réservé à l'appréciation du juge. La norme ne peut donc pas le faire.

➔ L'objectif est de ne pas amoindrir les preuves pré-existantes mais **rien n'est garanti** !

§ **nul ne peut se constituer une preuve à soi même**. Il s'ensuit que les informations collectées par le soin des équipes SSI seront souvent considérées comme des indices d'un événement, des commencement de preuve lorsque l'on cherche à leur conférer une valeur juridique. Mais elles resteront toujours vulnérables à une analyse minutieuse.

§ ce qu'en dit la **jurisprudence** :

Arrêt du **4 décembre 2008**, la Cour de cassation casse l'arrêt rendu par la Cour d'appel de Reims, notamment parce que celle-ci n'a pas recherché si un document produit en preuve par la CPAM de la Marne répondait aux exigences des articles 1334, 1348 et 1316-1 du code civil. La fidélité d'une copie, prétendant représenter un document daté de 2003 alors qu'elle provient de la réimpression d'un fichier numérique sous un logo n'ayant existé qu'en 2004. Avec la définition proposée par la norme Z42-013, la copie aurait été fidèle. Un logo d'organisme est un logo, qu'il soit de 2003 ou de 2004. En réimprimant le document à partir de données numériques, la CPAM n'a pas "reproduit" le titre original, mais qu'elle en a "reconstitué" l'information comme il est dit dans la définition de la norme.

Attendus de la Cour de cassation :

« **Qu'en statuant ainsi, sans rechercher si le document produit par la caisse pour justifier de l'accomplissement de la formalité prévue à l'article R. 441-11 du code de la sécurité sociale répondait aux exigences des articles susvisés, la cour d'appel a privé sa décision de base légale au regard de ces textes** »

Différents type d'acte requiert la constitution d'un dossier archivant des preuves :

§ contrat,

§ formulaire,

§ document de travail,

§ constats : cet how-to se concentre surtout sur ce type d'acte.

Le constat relatif au **contenu d'un site Internet**, notamment pour constater la présence de contenus illicites ou contestables. Pour quelles raisons ?

§ plagiat
§ protection des marques
§ atteinte à la vie privée (surtout avec le web 2.0)
§ diffamation

§ modification de contenu ou redirection par un pirate (hack)

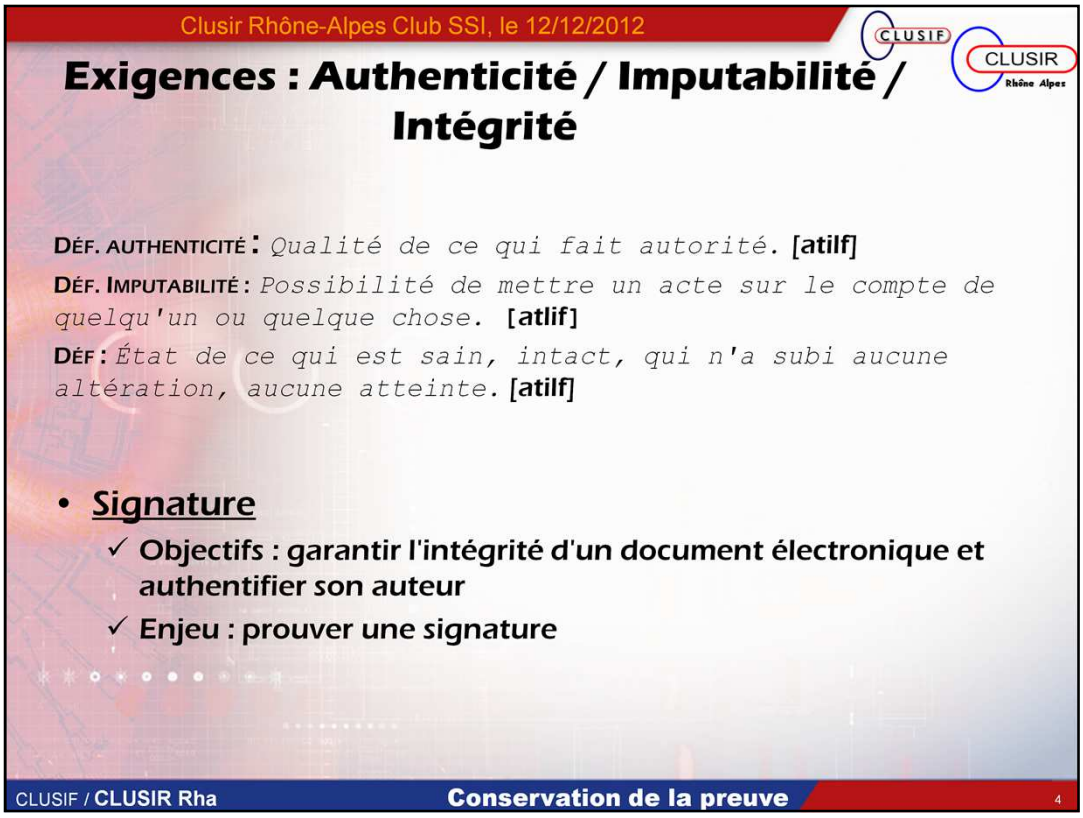
§ cybersquatting

§ spamdexing

§ DDoS

Le constat relatif à l'**émission ou la réception d'un mail**. Les courriers électroniques sont souvent utilisés devant les tribunaux en tant que **commencement de preuve** pour étayer un raisonnement juridique. En outre, elles peuvent servir de pièce justificative pour une transaction donnée ou un contrat.

➔ Être conscient que les éléments collectés seront souvent des commencements de preuves plus que des preuves. Pourquoi ? En partie parce que l'article **1316-4 du Code Civil** énonce que « *la signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle* ***confère l'authenticité*** *à l'acte.* »


Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Exigences : Authenticité / Imputabilité / Intégrité
DÉF. AUTHENTICITÉ : Qualité de ce qui fait autorité. [atilf]
DÉF. IMPUTABILITÉ : Possibilité de mettre un acte sur le compte de quelqu'un ou quelque chose. [atlif]
DÉF : État de ce qui est sain, intact, qui n'a subi aucune altération, aucune atteinte. [atilf]
• Signature
✓ Objectifs : garantir l'intégrité d'un document électronique et authentifier son auteur
✓ Enjeu : prouver une signature
CLUSIF / CLUSIR Rha
Conservation de la preuve
4

Authenticité, Imputabilité / Intégrité

Définition **Authenticité** : Qualité de ce qui fait autorité.

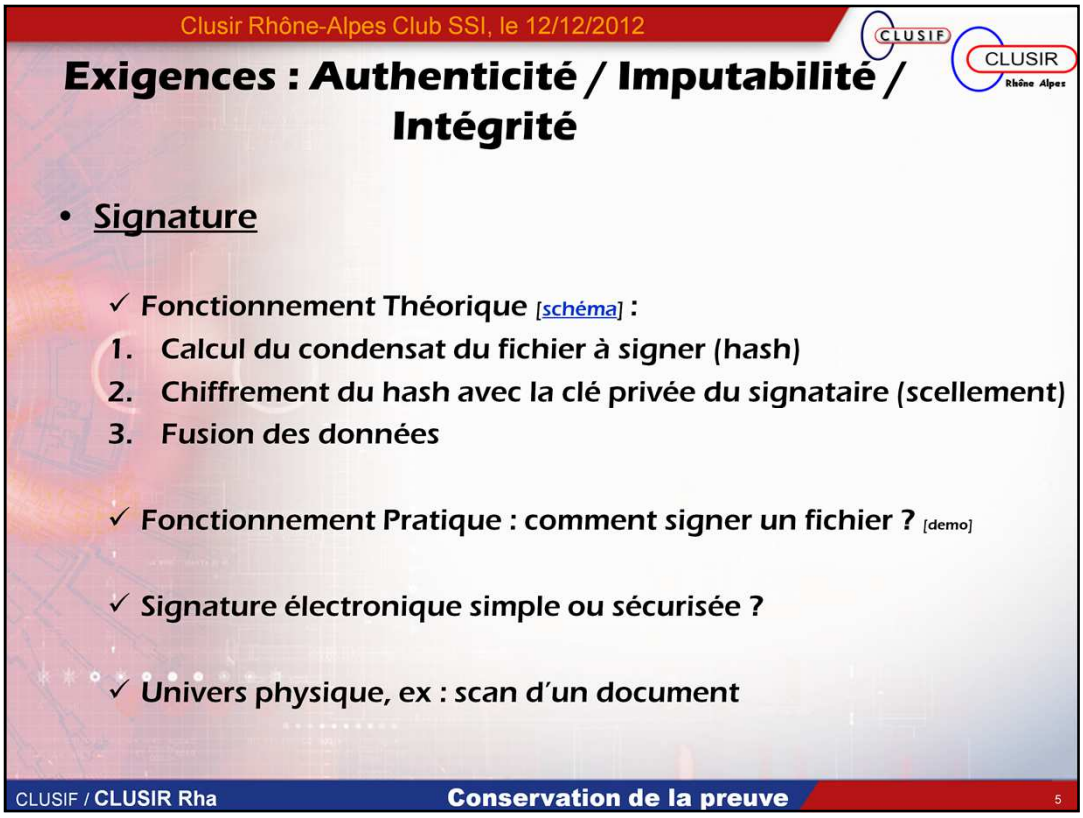
Imputabilité : Possibilité de mettre un acte sur le compte de quelqu'un ou quelque chose.

Intégrité : État de ce qui est sain, intact, qui n'a subi aucune altération, aucune atteinte.

Signature :

§ **Objectifs** : garantir l'intégrité d'un document électronique et authentifier son auteur

§ **Enjeu** : prouver une signature


Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Exigences : Authenticité / Imputabilité / Intégrité
• Signature
✓ Fonctionnement Théorique [schéma] :
1. Calcul du condensat du fichier à signer (hash)
2. Chiffrement du hash avec la clé privée du signataire (scellement)
3. Fusion des données
✓ Fonctionnement Pratique : comment signer un fichier ? [demo]
✓ Signature électronique simple ou sécurisée ?
✓ Univers physique, ex : scan d'un document
CLUSIF / CLUSIR Rha
Conservation de la preuve
5

Authenticité, Imputabilité / Intégrité

Signature :

§ **Fonctionnement Théorique** [schéma] :

1. Calcul du condensat du fichier à signer (hash), **STYLO**
2. Chiffrement du hash avec la clé privée du signataire (scellement), **CARTE D'IDENTITE**
3. Fusion des données

§ Logique :

- **possible** d'utiliser un certificat autosigné, valable uniquement pour les besoins de la constitution du dossier (ex 15 jours)

- Création d'une **clé auto-signée** :

* **openssl.exe req -new -newkey rsa:**4096 **-keyout** SashaPons-Forensic12122012.key **-out** SashaPons-Forensic12122012.csr **-days** 15

* **openssl.exe x509 -req -in** SashaPons-Forensic12122012.csr **-signkey** SashaPons-Forensic12122012.key **-out** SashaPons-Forensic12122012.cer -days 15

* **openssl.exe pkcs12 -export -in** SashaPons-

Forensic12122012.cer **-inkey** SashaPons-Forensic12122012.key **-out** SashaPons-Forensic12122012.pfx

- **Signature** numérique

* **openssl dgst -sha256 -sign** SashaPons-Forensic12122012.key **-out** fichier.sign fichier

* **openssl verify -CAFile** SashaPons-Forensic12122012.cer SashaPons-Forensic12122012.cer

* **openssl x509 -in** SashaPons-Forensic12122012.cer **-pubkey -noout >** SashaPons-Forensic12122012.pub

* **openssl dgst -sha256 -verify** SashaPons-Forensic12122012.pub **-signature** fichier.sign fichier

§ Conclusion ➔ pour **rendre intelligible** la signature à un être humain, il est nécessaire d'utiliser un logiciel de vérification de signature attestant ainsi de la validité de cette dernière. Actuellement seul le format PDF et des outils en ligne permette un rendu suffisant.

§ différence entre **signature électronique** et **signature électronique sécurisée** ?

Juridiquement, la signature électronique « simples », « sécurisées », ou utilisant des « certificats qualifiés » ont toutes la même valeur juridique. On met souvent en avant la « présomption de fiabilité », attachée aux signatures électroniques sécurisées réalisées selon le dispositif spécifié à l'article 1316-4, al. 2 du Code civil et à l'article 2 du décret du 30 mars 2001.

Il faut toutefois rappeler à ce sujet deux éléments :

* L'apport juridique de la signature « **emportant présomption de fiabilité** » est faible dans le cadre de relations B to B ou B to C.

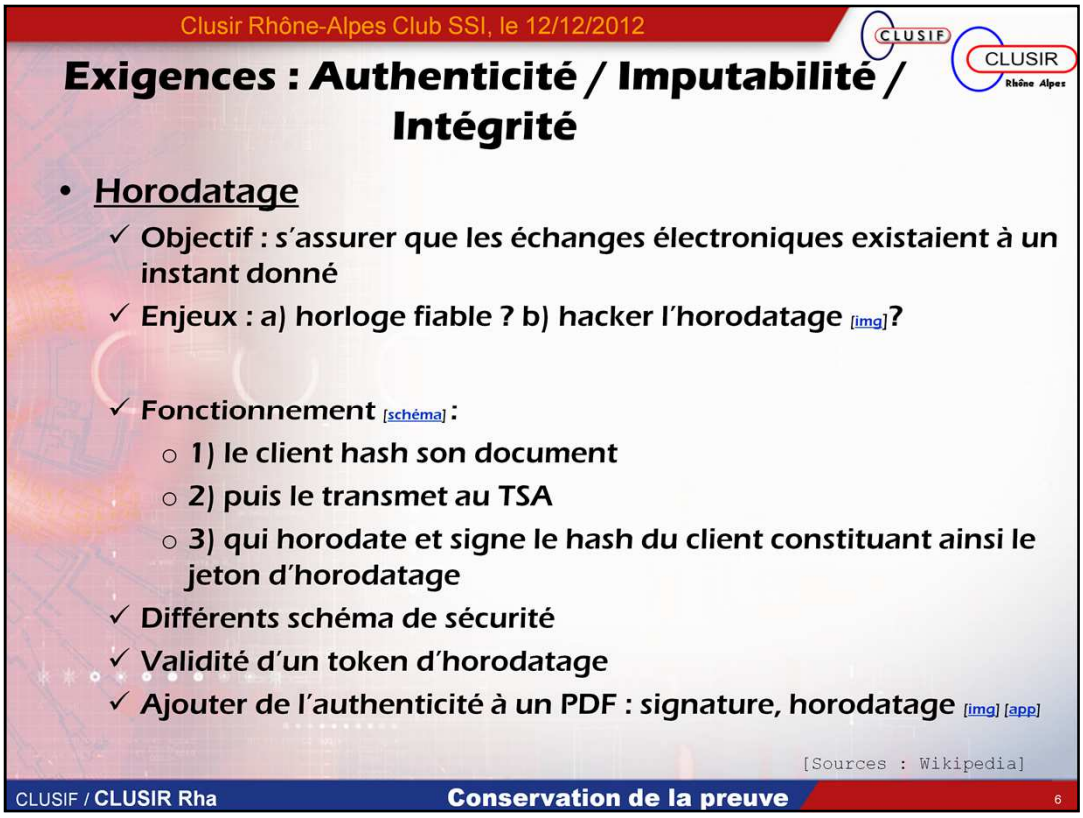
* Les exigences relatives à la signature sécurisée sont contraignantes à mettre en œuvre, et ne concerneront dans la pratique qu'une population très réduite, principalement les professions réglementées pour la perfection des actes authentiques.

➔ Conclusion : l'utilisation d'un **certificat auto-signé** est tout à fait correct pour les actions traitées dans cette présentation

§ Physique :

- Scanner : **REX sur MFP HP** :: Z42-013 demande de respecter de respecter la norme expérimentale XP Z42-012 (Imagerie électronique – Cibles de contrôle pour les systèmes de numérisation en noir et blanc des documents de bureau – Description et mode d'emploi). Difficile voir impossible car i) impossible d'obtenir l'**exhaustivité des informations techniques** (matériel et logiciel et

configuration) directement sur le MFP et ii) impossible de **régler finement les formats de fichier** (ex facteur de qualité pour la norme JPEG) ainsi que les résolutions.


Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Exigences : Authenticité / Imputabilité / Intégrité
Horodatage
Objectif : s'assurer que les échanges électroniques existaient à un instant donné
Enjeux : a) horloge fiable ? b) hacker l'horodatage [img] ?
Fonctionnement [schéma] :
1) le client hash son document
2) puis le transmet au TSA
3) qui horodate et signe le hash du client constituant ainsi le jeton d'horodatage
Différents schéma de sécurité
Validité d'un token d'horodatage
Ajouter de l'authenticité à un PDF : signature, horodatage [img] [app]
[Sources : Wikipedia]
CLUSIF / CLUSIR Rha
Conservation de la preuve
6

Authenticité, Imputabilité / Intégrité

Définition : Qualité de ce qui fait autorité.

Horodatage :

§ littéralement, c'est la **contraction** de date et heure. L'objectif est de **s'assurer que les échanges électroniques existaient à un instant donné**. Pour s'assurer que l'antidatage et le postdatage ne sont pas possible. Le plus gros **tiers horodateur** c'est la Poste : cachet de la poste faisant foi ou envoi en recommandé ; seul la vérification du courrier peut-être litigieuse dans ce cas.

§ Problème :

- est-ce que l'heure et la date de l'horloge sont correctes ? horloge fiable : NTP, STIME pas normé.

- peut-on pirater un jeton d'horodatage ? Tout l'enjeux des algorithmes utilisés. Détail :

§ Principe de fonctionnement :

1) le client hash son document

2) puis le transmet au TSA

3) qui horodate et signe le hash du client constituant ainsi le jeton d'horodatage

➔ la fonction d'horodatage met en œuvre un **certificat** électronique d'un type particulier, appelé token.

§ Différents schémas de sécurité :

- basé sur une **PKI** et donc sur la **signature digitale**. Problématique habituelle de confiance.

- **hash-linking**, le jeton d'horodatage est généré à partir d'information contenues dans le précédent jeton délivré.

- distribués : plusieurs TSA sont contactées, le jeton étant délivrés en incluant toutes les informations. Réduit les risques si le TSA est compromis.

- …

§ Comment contrôler la **validité** d'un token d'horodatage ?

1) validité de la signature du token au regard du certificat de la TSA ;

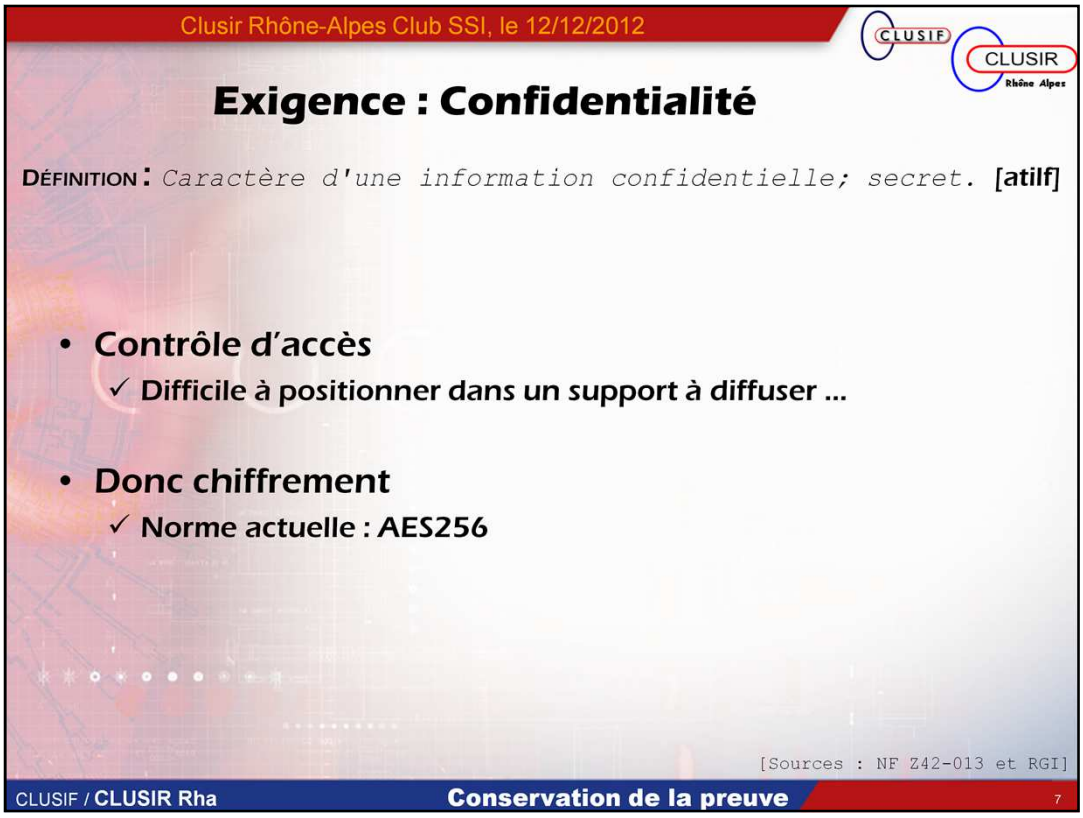
2) validité du certificat du TSA (trustChain) ;

3) validité du hash scellé vis-à-vis du hash calculé dans le document ;

§ **Universign** (Société cryptolog) est visiblement la seule autorité d'horodatage française (Time Stamping Authority) qualifiée RGS. Tarifs : 0,40€ par signature. Service d'envoi d'un mail en Cci pour horodatage. Le mail est retourné au format eml ainsi que le jeton d'horodatage au format ERS. Peu d'outils permettent de **vérifier le token** d'horodatage ainsi délivré (contrairement à ce qui est dit) => PDF reste le client permettant de produire et de vérifier le plus facilement un token d'horodatage.

§ Il est possible de signer et horodater ses fichiers PDFs en utilisant l'imprimante PDF Creator. DEMO.

§ Lorsque les fichiers sont **trop volumineux**, le plus simple est d'en faire le hash, de le copier dans un fichier txt, de l'imprimer en PDF avec signature.

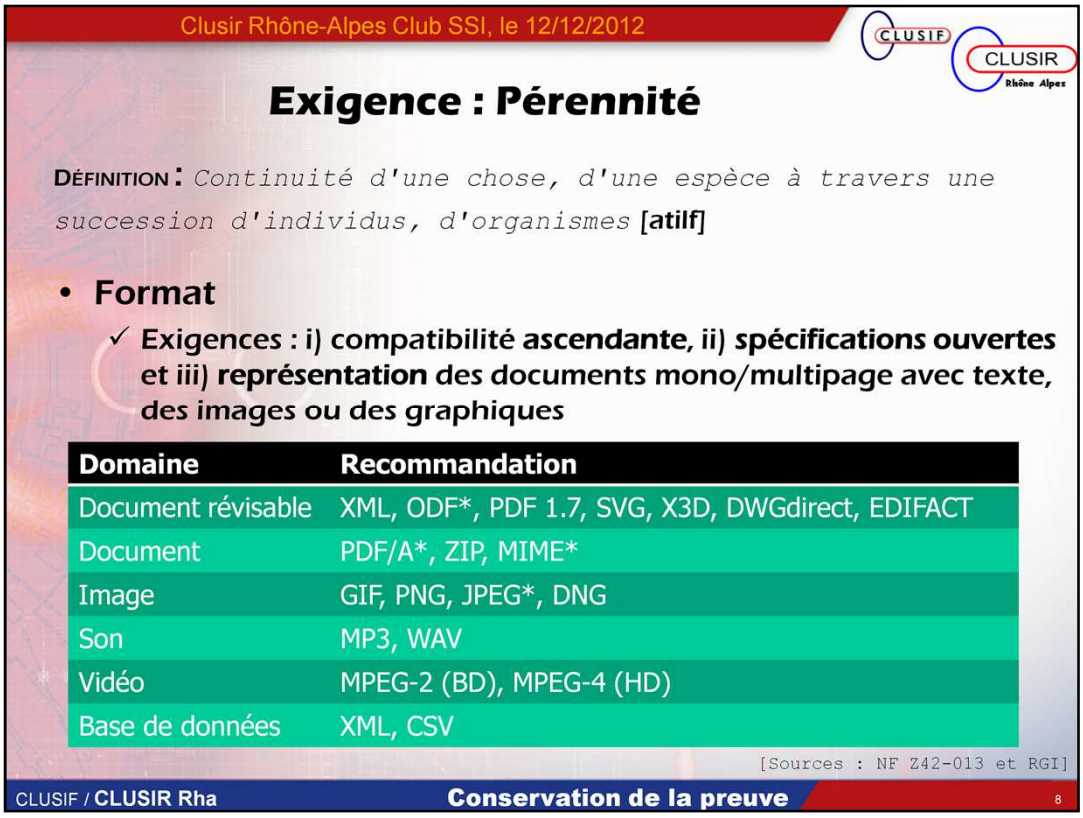

Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Exigence : Confidentialité
DÉFINITION : Caractère d'une information confidentielle; secret. [atilf]
• Contrôle d'accès
✓ Difficile à positionner dans un support à diffuser ...
• Donc chiffrement
✓ Norme actuelle : AES256
[Sources : NF Z42-013 et RGI]
CLUSIF / CLUSIR Rha
Conservation de la preuve
7

Confidentialité

Définition : Caractère d'une information confidentielle; secret.

Caractère d'une information confidentielle; secret;

-> ACL – lié au système de fichier, peut être contourné et Chiffrement


Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Exigence : Pérennité
DÉFINITION : Continuité d'une chose, d'une espèce à travers une succession d'individus, d'organismes [atilf]
• Format
✓ Exigences : i) compatibilité ascendante, ii) spécifications ouvertes et iii) représentation des documents mono/multipage avec texte, des images ou des graphiques
Domaine | Recommandation
Document révisable | XML, ODF*, PDF 1.7, SVG, X3D, DWGdirect, EDIFACT
Document | PDF/A*, ZIP, MIME*
Image | GIF, PNG, JPEG*, DNG
Son | MP3, WAV
Vidéo | MPEG-2 (BD), MPEG-4 (HD)
Base de données | XML, CSV
[Sources : NF Z42-013 et RGI]
CLUSIF / CLUSIR Rha
Conservation de la preuve
8

Pérennité

Définition : Continuité d'une chose, d'une espèce à travers une succession d'individus, d'organismes

Définitions connexes :

§ **lisibilité**, fait qu'une écriture, un texte imprimé soit facilement perçu lors de la lecture

§ **disponibilité**, fait de pouvoir être rapidement utilisé, d'être à la disposition de quelqu'un.

Dans le cadre de cet How-To, je ne fais volontairement pas de différence entre le format de **conservation** et le format de **diffusion** pour éviter toutes les problématiques liées à la migration du format de donnée (cas par exemple d'une bibliothèque mettant à disposition du contenu multimédia archivé en streaming). La diffusion se fait dans le format de conservation.

Format

§ Exigences z42-013

AFNOR dit que le format doit respecter i) une **compatibilité ascendante**, ii) des **spécifications ouvertes** et iii) possibilité de représenter les documents mono ou

multipage mélangeant du **txt**, des **images** ou des **graphiques**.

§ Sources : NF Z42-013 et RGI. Le croissement de ces 2 normes permet de répondre aux 3 critères ci-dessus.

§ /!\ DOC n'est pas reconnu par la norme ISO /!\

§ Sûr, mais pas listé dans la version de 2001, PDF/A. /!\ bien sélectionner ce format par défaut dans la configuration de l'imprimante PDF /!\. Sûr car publication en octobre 2012 de la norme internationale **ISO 19005-3 (PDF/A-3).** PDF est **propriété d'Adobe** mais a toujours été publié ➔ exception ;-). De plus, **http://www.crackmypdf.com/** permet d'enlever les protections d'un PDF chiffré trop faiblement.

§ L'**exportation** de mail depuis **Outlook** ne peut pas se faire au format MIME, mais seulement MSG, propriétaire. Nécessite d'utiliser un script perl (ex msgconvert.pl).

§ le JPG est destructeur. Utiliser JPEG2000 comme format pour les photos. Sinon, privilégiez les formats vectoriels.

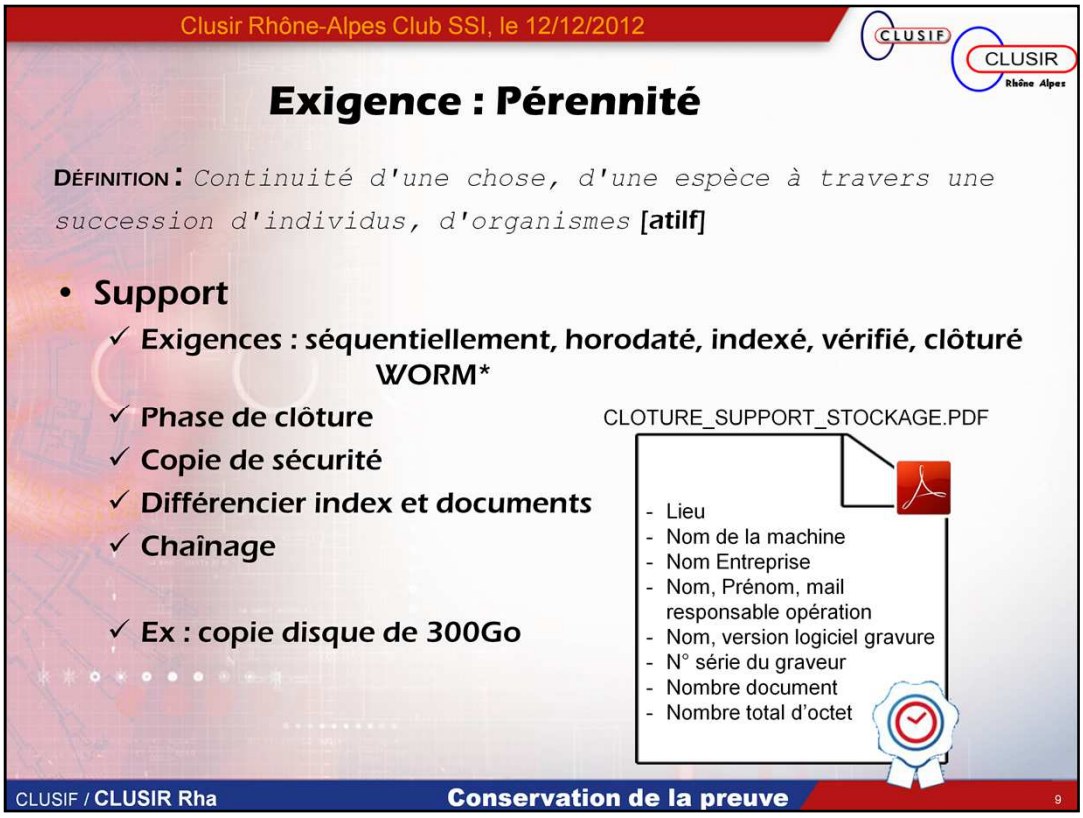
§ Scan de document : **400 dpi** et d'abandonner le noir et blanc au profit du **niveaux de gris** (sauf cas particulier où le rendu d'une illustration est meilleur en noir et blanc). JPEG2000 en format d'archivage. Source -> http://www.bnf.fr/pages/infopro/numerisation/pdf/formats_images.pdf

§ plus les formats sont simples, plus ils seront faciles à migrer.

§ inclure les **légendes** des données du fichier (dans un fichier à part, recevant le même traitement que le fichier de donnée) de log par exemple si l'exportation en fichier TXT ne les positionnent pas dans les headers.

§ NF Z42-013, dans sa version de 2001, **exclues** le stockage des fichiers **sons**, **films** ainsi que les fichiers d'**imagerie médicale**. Est-ce mis à jour dans la nouvelle version ?

§ **Format ERS** : actuellement décrit dans un draft d'une RFC (draft-ietf-ltans-xmlers-11.txt). Enveloppe pouvant contenir de l'ASN1 ou du XML (XMLERS). Standardisation notamment pour l'archivage à long term.


Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Exigence : Pérennité
DÉFINITION : Continuité d'une chose, d'une espèce à travers une succession d'individus, d'organismes [atilf]
• Support
✓ Exigences : séquentiellement, horodaté, indexé, vérifié, clôturé
WORM*
✓ Phase de clôture
✓ Copie de sécurité
✓ Différencier index et documents
✓ Chaînage
✓ Ex : copie disque de 300Go
CLOTURE_SUPPORT_STOCKAGE.PDF
- Lieu
- Nom de la machine
- Nom Entreprise
- Nom, Prénom, mail responsable opération
- Nom, version logiciel gravure
- N° série du graveur
- Nombre document
- Nombre total d'octet
CLUSIF / CLUSIR Rha
Conservation de la preuve
9

Pérennité

---

support :

§ Attention aux CD/DVD, choisir des supports à métallisation or, gravé à 90% de capacité, à vitesse moyenne, en double exemplaires stockés dans des lieux distincts. Contrôles tous les 5 ans.

§ Clôture :

- doit comporter le **lieu** de l'initialisation avec, éventuellement, une **adresse** électronique de la machine sur laquelle s'effectue cette initialisation ;

- **l'horodatage** de cette initialisation ;

- le nom de l'organisme ou de l'**entreprise** ;

- le nom, prénom, mail du **responsable** de l'opération ;

- le nom et la version du **logiciel** qui a servi à formater le disque ;

- le **numéro de série** du lecteur enregistreur qui a servi à formater le disque ;

- le **nombre de documents** produits par l'utilisateur et stockés sur le support ;

- le **nombre total d'octets** que représentent les documents de l'utilisateur (avant et après compression)

- certaines des informations ci-dessus peuvent être mise dans les métadata du CD/DVD

§ **Copie de sécurité**

- à indexer dans la main courante en incluant la personne à qui elles sont transmises

- ne pas utiliser la même série de CD que les originaux

§ Différencier la sauvegarde des **documents** et des **index** répertoriant ces documents.

§ /?\ NF Z 42-013-> Parfois les conditions de conservation ne peuvent être respectées, faute de moyens : pas de double lieu de stockage, de copies régulières et transferts de supports

§ **Chaînage** : opération consistant par exemple à graver 20Go sur des DVD. Chaque portion de l'archive doit référencer la précédente et la suivante dans un tableau de correspondance incluant la numéro de série du disque utilisé. Les médias correspondants aux copies de sécurité doivent référencer non pas les autres copies de sécurité, mais bien les médias originaux.

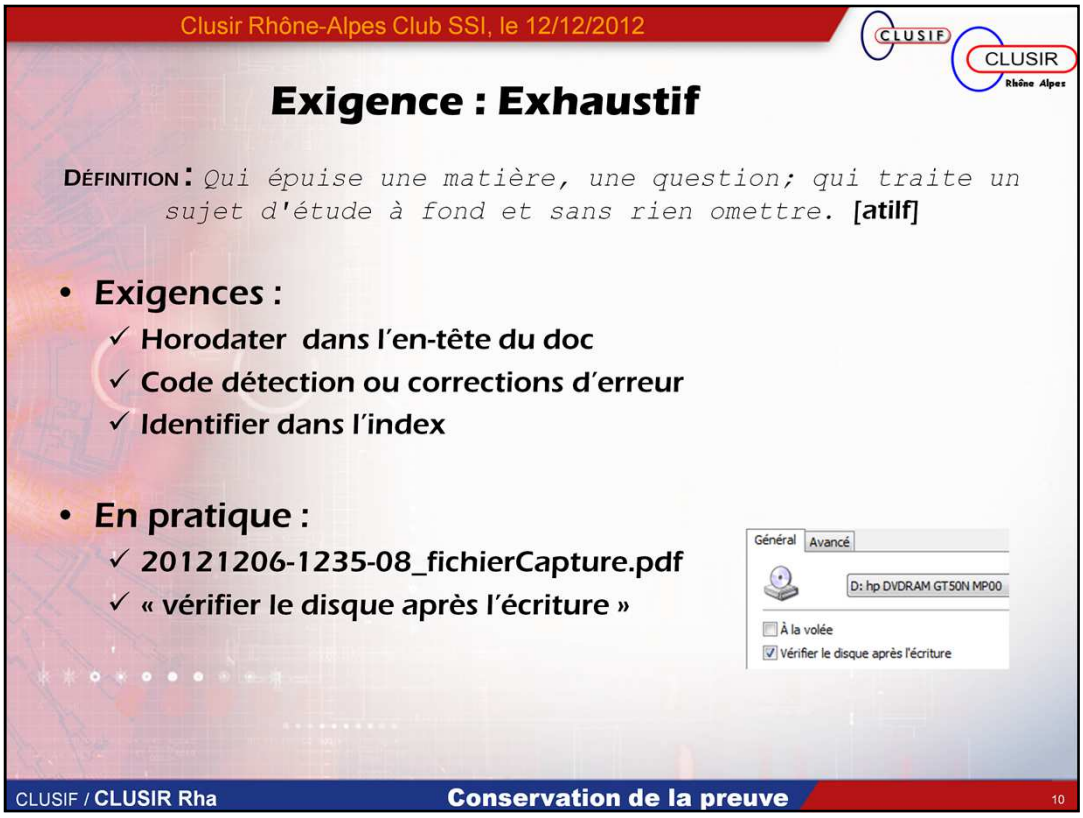
§ **Transfert sur support de stockage** : Exemple d'un disque dur d'ordinateur de 300Go

- sur DVD : 67 DVD à graver pendant plus de 24h :-/

- sur Blu-ray : 6 blu-ray pendant 1h45

- le temps de constituer les archives chiffrées d'une taille correcte pour être gravées : ZIP, splitté pour DVD, chiffré en AES256 -> 50h sur un petit portable :-/

§ **Copie de disque dur** : alternative permettant aussi d'analyser des secteurs défectueux et de faire du forensic lors de la copie. Voici une ressource listant les solutions existantes : http://www.jharddrive.com/


Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Exigence : Exhaustif
DÉFINITION : Qui épuise une matière, une question; qui traite un sujet d'étude à fond et sans rien omettre. [atilf]
• Exigences :
✓ Horodater dans l'en-tête du doc
✓ Code détection ou corrections d'erreur
✓ Identifier dans l'index
• En pratique :
✓ 20121206-1235-08_fichierCapture.pdf
✓ « vérifier le disque après l'écriture »
Général
Avancé
D: hp DVDRAM GT50N MP00
À la volée
Vérifier le disque après l'écriture
CLUSIF / CLUSIR Rha
Conservation de la preuve
10

Exhaustif

Définition : Qui épuise une matière, une question; qui traite un sujet d'étude à fond et sans rien omettre.

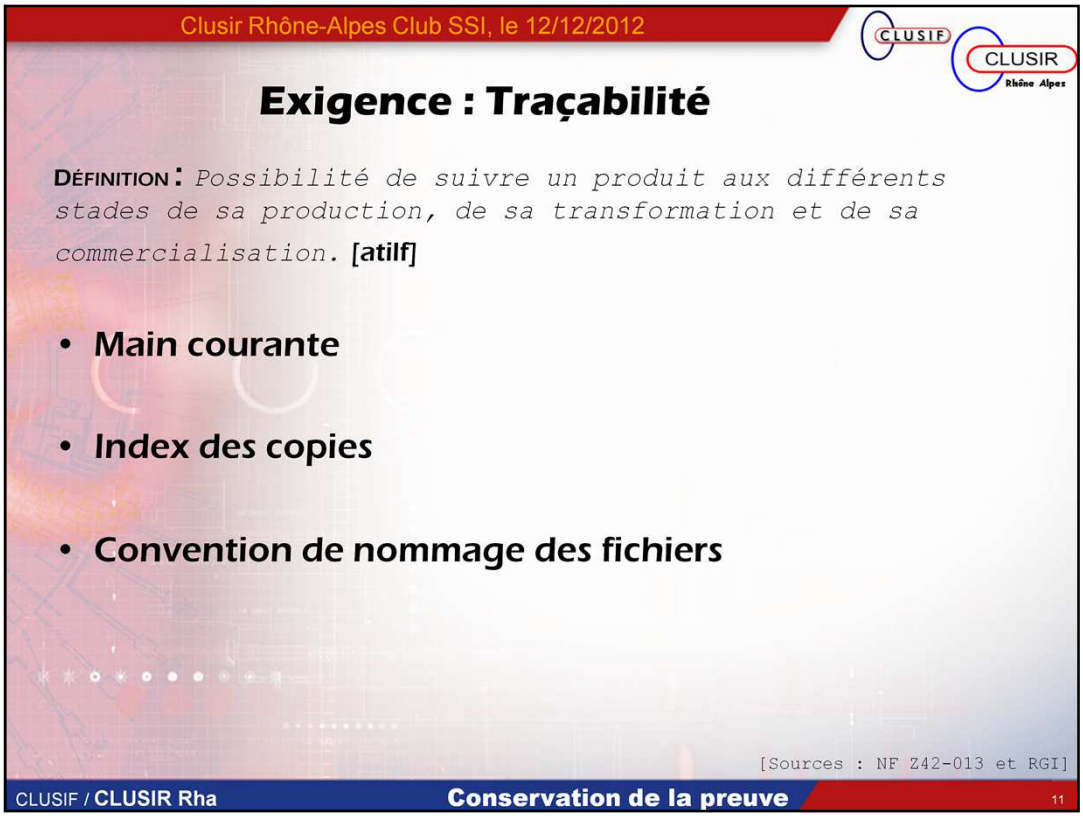
Exigences : - date/heure de l'enregistrement du document dans l'en-tête du fichier ou à défaut dans la main courante ;

- vérifier que l'enregistrement est OK grâce aux codes de détection ou de corrections d'erreur

- confirmer que l'enregistrement a été identifié par l'index

-> hash du répertoire, mise dans une archive et hash de l'archive ?

§ Nomenclature : en suivant les exigences notamment de NF Z42-013, voici une nomenclature adaptée : 20121206-1235-08_fichierCapture.pdf

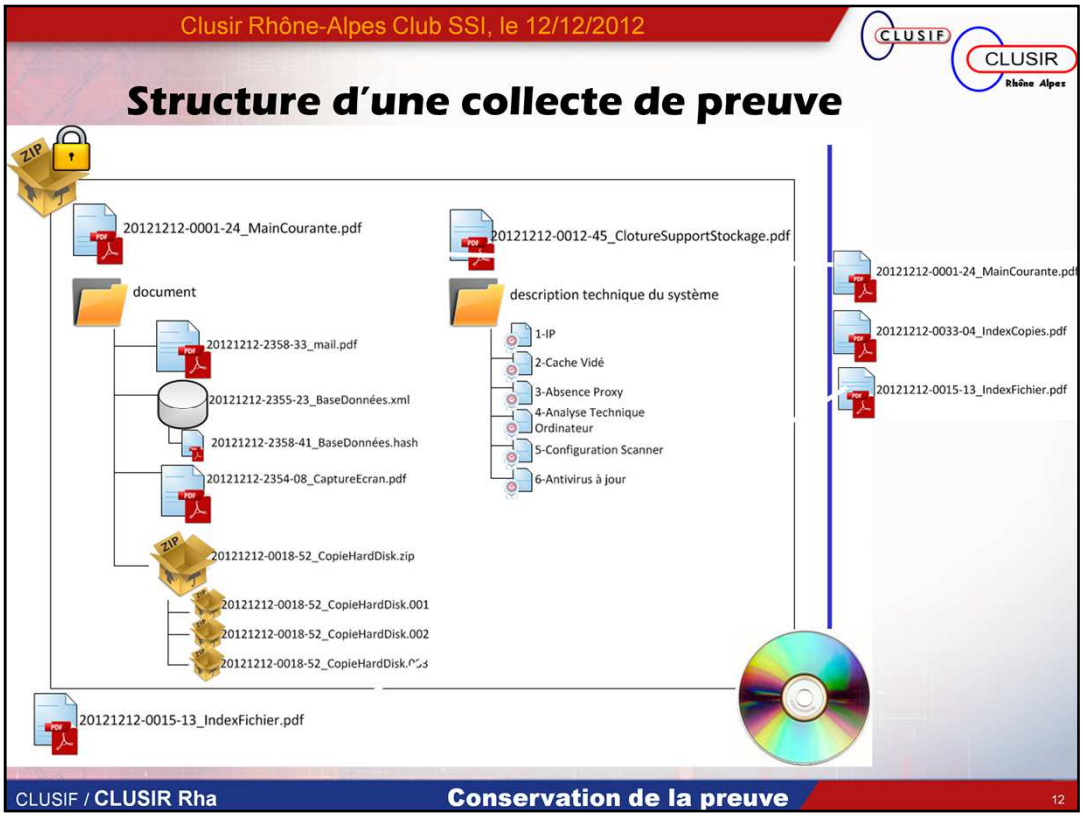

Clusir Rhône-Alpes Club SSI, le 12/12/2012
CLUSIF
CLUSIR
Rhône Alpes
Exigence : Traçabilité
DÉFINITION : Possibilité de suivre un produit aux différents stades de sa production, de sa transformation et de sa commercialisation. [atilf]
• Main courante
• Index des copies
• Convention de nommage des fichiers
[Sources : NF Z42-013 et RGI]
CLUSIF / CLUSIR Rha
Conservation de la preuve
11

Traçabilité

Définition : Possibilité de suivre un produit aux différents stades de sa production, de sa transformation et de sa commercialisation.

-> enregistrer dans un journal (main courante) les opérations effectuées sur les documents, archivage de ce journal.

-> NF Z42-013 indique que les historiques des événements doivent être horodatés



Structure d'une collecte de preuve

Voici présenté schématiquement les conclusions de toutes les exigences de sécurité listées dans cette présentation.